PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 11/30, 12/14 — A1

(11) International Publication Number: WO 93/09495

(43) International Publication Date: 13 May 1993 (13.05.93)

(21) International Application Number: PCT/AU92/00594

(22) International Filing Date: 5 November 1992 (05.11.92)

(30) Priority data:
PK 9297 5 November 1991 (05.11.91) AU

(71) Applicant *(for all designated States except US)*: AUSTRALIAN TECH SUPPORT PTY. LTD. [AU/AU]; 717 Gympie Road, Lawnton, QLD 4501 (AU).

(72) Inventor; and

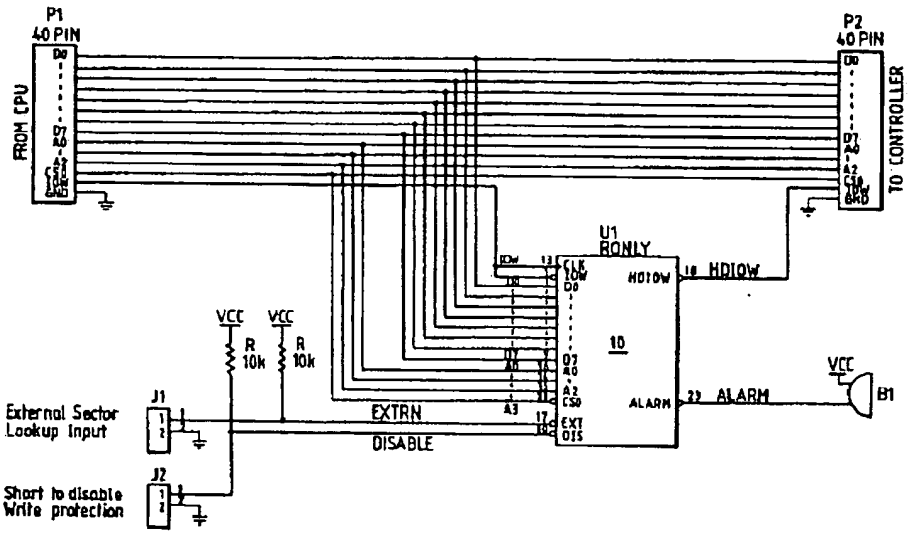
(75) Inventor/Applicant *(for US only)* : ROGERS, Thomas, Joseph [GB/AU]; 45 Hedge Street, Strathpine, QLD 4500 (AU).

(74) Agent: CULLEN & CO.; 240 Queen Street, Brisbane, QLD 4000 (AU).

(81) Designated States: AU, CA, JP, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, SE).

Published
With international search report.

(54) Title: COMPUTER MEMORY PROTECTION



(57) Abstract

A write protection device (10) prevents data from being written to selected portions of the hard disc of a computer. The write protection device is connected between the CPU of the computer and the controller for the hard drive. The write protection device monitors the read/write commands from the CPU to the controller. The address of each write command is compared with preselected address(es) stored in registers (12, 15) corresponding to the partition area and boot sector, and/or any other preselected address listed in a look-up table (160). In the event of a positive comparison, the write command is prevented from reaching the controller. Individual sectors of the disc can be write protected while still permitting writing to other sectors, even within the same cylinder. Low level format commands can be detected and disabled separately from write commands.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FR	France	MR	Mauritania
AU	Australia	GA	Gabon	MW	Malawi
BB	Barbados	GB	United Kingdom	NL	Netherlands
BE	Belgium	GN	Guinea	NO	Norway
BF	Burkina Faso	GR	Greece	NZ	New Zealand
BG	Bulgaria	HU	Hungary	PL	Poland
BJ	Benin	IE	Ireland	PT	Portugal
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SK	Slovak Republic
CI	Côte d'Ivoire	KZ	Kazakhstan	SN	Senegal
CM	Cameroon	LI	Liechtenstein	SU	Soviet Union
CS	Czechoslovakia	LK	Sri Lanka	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	MC	Monaco	UA	Ukraine
DK	Denmark	MG	Madagascar	US	United States of America
ES	Spain	ML	Mali	VN	Viet Nam
FI	Finland	MN	Mongolia		

"COMPUTER MEMORY PROTECTION"

THIS INVENTION relates to computer security. In particular, the invention is directed to a method and apparatus for preventing the unauthorised writing of data to selected portions of a memory device, such as a hard disc of a computer. The invention is particularly useful for preventing "virus" programmes becoming resident in a computer memory device.

BACKGROUND OF THE INVENTION

So-called "virus" computer programmes, or more simply "viruses", are unwanted programmes which are designed to interfere with the normal or intended operation of a computer. Although some viruses may only be mischievous in their operation, many viruses are written with malicious intent to cause serious damage, for example by destroying valuable data on a hard disc or otherwise rendering such data irretrievable. The damage caused by such computer viruses can be catastrophic.

Any virus, regardless of its effect, is a threat to the security of a computer system. Significant costs and downtime are incurred in searching for, and eradicating, virus programmes which may have found their way into a computer memory, and replacing lost data and programmes. With the increasing prevalence and variety of virus programmes in recent years, viruses pose a serious threat to all computer systems, large or small.

Various virus detection techniques have been proposed. Such techniques are normally software-based. Typically, an anti-virus programme attempts to detect the presence of a virus in a computer memory, such as a hard disc, by searching for a characteristic string of binary digits which identifies the virus. However, such software techniques are not effective for all known viruses. Further, some virus programmes are known to "mutate" and alter their characteristic string, thereby making such programmes virtually undetectable using conventional software techniques.

Another known anti-virus programme seeks to foil the intended operation of the virus by trapping interrupt commands. However, this known programme is not always effective against some viruses, and completely ineffective against others.

U.S. patent no. 5,144,660 (and its equivalent Australian patent application no. 40095/89) describes a method of securing a computer against undesired write operations to, or read operations from, a hard disc of the computer in order to protect the computer against viruses. This method involves interposing logic circuitry between the disc controller and the read/write head(s) of the disc drive, decoding control signals between the controller and the disc drive and, in response to such decoding, controlling the write or read operations from the disc drive.

However, the protection technique taught by U.S. patent no. 5,144,660 has several inherent disadvantages. First, since the logic circuitry is interposed between the controller and the hard disc, it is only possible to read or write protect whole cylinders on the disc. That is, it is not possible to differentiate between sectors within a particular cylinder on the disc. For example, cylinder 0 head 0 sector 1 of the disc normally contains a partition table and the rest of the sectors are not used. The prior art system requires that all sectors on the cylinder be protected even though only one sector is required to be protected as a precaution against virus programmes. Further, cylinder 0 head 1 sector 1 is normally allocated to the master DOS boot record, while cylinder 0 head 1 sector 2 is normally the file allocation table. Although it may be desired to protect the master DOS boot record but not the file allocation table, the prior art method and apparatus does not permit such differentiation within a cylinder.

Secondly, the prior art method and apparatus

are not suitable for computer systems in which the disc controller and the read/write head(s) are formed as a single unit.

Thirdly, since separate cables are provided for control and data signals, the protection apparatus of U.S. patent no. 5,144,660 requires a counter to track the particular cylinder being addressed.

Fourthly, the prior art protection apparatus cannot differentiate between signals sent by the CPU to the disc controller, e.g. between write commands and "low level" format commands. As the write protection device was positioned between the controller and the disc, it was impossible to tell whether the controller was writing data or doing a low level format command as both give the same signals leaving the controller.

It is an object of the present invention to provide improved apparatus and method for preventing unwanted information, data or programmes, such as viruses, being written to a data storage device of a computer.

SUMMARY OF THE INVENTION

In one broad form, the present invention provides apparatus for preventing the unwanted writing of data to selected portion(s) of a memory device of a computer having a CPU and a controller for the memory device, the apparatus comprising a write protection device having

memory means containing the address(es) of selected portion(s) of the memory to which data is not intended to be written;

decoding means for reading the address of any write command to the memory device;

comparator means for comparing the write address with the address(es) of the selected portion(s) and

disabling means responsive to the output of the comparator means for disabling the write

command,

characterised in that the write protection device is connected between the CPU and the controller.

Preferably, the decoding means also detects low level format commands and these are stopped in the same manner as write commands to protected sectors.

In another form, the present invention provides a method of preventing unwanted writing of data to selected portion(s) of a memory device of a computer having a CPU and a controller for the memory device, comprising the steps of

(a) selecting the portion(s) of the memory device to which data is not intended to be written and storing the address(es) of the portion(s),

(b) reading the address of any write command from the CPU to the controller,

(c) comparing the write address with the stored address(es) of the preselected portion(s), and

(d) disabling those write commands having an address corresponding to the preselected portion(s),

characterised in that steps (b)-(d) are performed by a write protection device connected between the CPU and the controller.

Preferably, low level format commands are also detected and disabled.

The term "data" is intended to include any information or program which may be stored in electronic or magnetic format in the memory device.

Typically, the memory device is the hard disc of a computer, but may be any other sectored or addressable non-volatile memory device, such as a laser disc, floppy disc, RAM, etc.

As the memory is write protected by hardware means, the security system cannot be overwritten or circumvented by software.

By using hardware to physically prevent the writing of data to preselected portions of the memory

device, those portions of the memory device effectively become read-only-memory, permitting data to be read but not written thereto. Since all data will be prevented from being written to the preselected portions of the storage device, viruses will be thwarted, regardless of their particular composition or mode of operation, as such viruses will not be able to become resident in the preselected portions of the memory device.

A particular advantage of the present invention is that individual portions of the memory device corresponding to specific addresses can be protected separately. Thus, if the memory device is a hard disc, individual sectors in a particular cylinder can be protected. The logic circuitry detects any attempt to write a particular sector by decoding the write address and comparing it with stored addresses of sectors to be write protected. If an attempt is made to write to a "protected" sector, the write command will be disabled, i.e. the write command will be prevented from reaching the controller or otherwise rendered ineffective. However, if an attempt is made to write to a sector which is not protected, the write command will be permitted to be executed even though that sector may be in the same cylinder as a protected sector.

A virus programme normally is transferred to the boot sector of a hard disc of the computer, typically when the computer is switched on with a floppy disc (having the virus programme) inserted in a disc drive of the machine. In the preferred embodiment of this invention, the boot sector, and all the sectors in the partition area, are permanently write barred. That is, these portions of the hard disc of the computer would normally always be selected to prevent the writing of any data or programme thereto.

If other portions of the memory device are to be write barred, the addresses of these portions can be stored in a look-up table, e.g. in non-volatile memory.

The address of any write command can then be compared also with the addresses in the look-up table to ascertain whether the write command will be carried out.

Since the write protection device of this invention is inserted between the CPU and the controller, it has the advantage of being able to selectively prevent other commands, such as low level format commands from being executed.

In order that the invention may be more fully understood and put into practice, a preferred embodiment thereof will now be described with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a circuit diagram illustrating the write protection circuit of an embodiment of this invention connected to a computer system;

Fig. 2 is a circuit diagram of part of the write protection circuit of Fig. 1 for fixed memory portions; and

Fig. 3 is a circuit diagram of part of the write protection device of Fig. 1 for selectable memory portions.

DESCRIPTION OF PREFERRED EMBODIMENT

The write protection circuit of the illustrated embodiment monitors all commands sent to the controller for the memory or storage device, typically a hard disc. These commands will move the read/write head or other mechanism to a particular portion of the storage device, e.g. to a particular sector of the hard disc. In particular, the write protection device detects write and format commands.

The write protection device tracks these sector commands and compares the write addresses with preselected addresses and/or addresses in a look-up table to determine whether a write command is permissible. If the write address corresponds to a preset sector or a sector listed in the look-up table, the write protection

circuit disables the write command, e.g. by not permitting the command to reach the storage device. Low level format commands are also disabled. All read commands however, are unaffected.

As illustrated in the drawings, particularly Fig. 1, the write protection device 10 can be mounted on a card and interconnected between the CPU and the controller of the hard disc (or other storage device) of a computer. Plug-in and/or piggy-back connections connected to the input and output of the card allow quick and simple installation in the computer.

The write protection device taps into the memory data bus to monitor the commands from the CPU to the controller for the hard disc. These commands may include read, write, format, recalibrate, verify, reset and identify commands. The recalibrate, write, format and reset commands are detected. A sector within the hard disc is selected by writing values to registers in the hard drive controller to select a particular read/write head, a track or cylinder, and the required sector on that cylinder.

As shown more specifically in Fig. 2, the commands on the data bus are tracked by an instruction decoder 11 which detects any write or low level format commands and provides the appropriate output. The commands are also fed to registers 12-15 which have been preset to detect preselected values. In the illustrated embodiment, these values correspond to all sectors in the partition area, and the boot sector, of the hard disc. (The partition area is cylinder 0, head 0 and all the sectors on that cylinder/head. The boot sector is cylinder 0, head 1, sector 1).

If the sector of the command address fed to registers 12-15 corresponds to one of the preset sector addresses representing the partition area or boot sector, the output of AND gate 2 or AND gate 3 will be high, and hence the output of OR gate 4 will also be high. The

output of the OR gate 4 is ANDed with the WRITE command output from the instruction decoder 11 by AND gate 5.

The output of AND gate 5 is inverted by inverter 9, and ANDed with the system write command by AND gate 6, the output (HDIOW) of which is fed to the device controller. Thus, if the command address corresponds to one of the preset addresses in latches 12-15, the write command will be prevented from reaching the device controller.

If the output of AND gate 5 goes high, an alarm 8 is triggered by flip-flop 7 indicating that an attempt has been made to write to a protected area of the disc. Once the alarm 8 has been triggered the output $\overline{Q}$ of flip-flop 7 is latched low and all write commands are stopped by AND gate 6 regardless of their drive or sector. This acts as a fail safe to prevent further damage once the protected sectors are threatened.

Jumper switch J2 is connected to the input of AND gate 5 to effectively short out the write protection mechanism, e.g. if it is desired to write to the protected areas. The jumper switch J2 may suitably be key operated.

If other sectors of the hard disc are to be write barred, the head/cylinder/sector addresses of such sectors can be stored in a look-up table in non-volatile memory, such as an EPROM, EEPROM, or static RAM with battery backup, connected to the OR gate 4 via jumper switch J1. As illustrated in Fig. 3, a one Mbyte EEPROM 160 is provided to store the locations of the sectors to be write protected. These sectors can be varied by reprogramming the EEPROM 160.

Each command address is compared with the addresses of the preselected sectors using suitable comparator means, such as a programmable logic array. The output of the comparison is fed via J1 to the input of OR gate 4. Thus, if the command address corresponds to either the partition area or boot sector or any other

preselected address listed in the look-up table 160, the output of AND gate 5 will be high and the output of AND gate 6 (to the controller) will be low, and hence the write command (IOW) from the CPU will be effectively prevented from reaching the device controller.

Both the output of AND gate 5 and the FORMAT COMMAND output of decoder 11 are connected to OR gate 10, the output of which is connected to invert 9 and the alarm 8. In this manner, any low level format command to any physical drive connected to the controller will be prevented from reaching the hard disc controller, and will also trigger the alarm 8. The write protection device of the illustrated embodiment can therefore protect against low level format commands while still allowing write commands.

In summary, the write protection device of the illustrated embodiment monitors the read/write commands in parallel with the hard disc controller and will normally allow all commands to reach the controller. However, when a write command is issued, and the read/write heads have been positioned to the restricted sectors, the write command will be prevented from reaching the controller, thereby preventing writing to the protected sectors. Low level format commands can also be blocked separately from write commands.

A particular advantage of the write protection system is that as there is no overhead in time required to check the validity of the write command, there is no degradation in performance.

As the write protection device is based wholly on hardware, it can be adapted to any software operating system.

The foregoing describes only one embodiment of the invention, and modifications which are obvious to those skilled in the art may be made thereto without departing from the scope of the invention as defined in the following claims. For example, although the write

protection device has been described with particular reference to a hard disc, it can be used to protect any memory system based on a sector type format.

The decoder 11 can also be modified to detect other selected commands to be disabled.

CLAIMS:

1. Apparatus for preventing the unwanted writing of data to selected portion(s) of a memory device of a computer having a CPU and a controller for the memory device, the apparatus comprising a write protection device having

memory means containing the address(es) of selected portion(s) of the memory to which data is not intended to be written;

decoding means for reading the address of any write command to the memory device;

comparator means for comparing the write address with the address(es) of the selected portion(s) and

disabling means responsive to the output of the comparator means for disabling the write command,

characterised in that the write protection device is connected between the CPU and the controller.

2. Apparatus as claimed in claim 1, wherein the memory device is a hard disc drive.

3. Apparatus as claimed in claim 2, wherein the addresses of the partition area and the boot sector of the hard disc are preset in the memory means.

4. Apparatus as claimed in claim 3, wherein the memory means further comprises a look-up table and the addresses of further portions of the hard disc which are to be write protected are stored in the look-up table.

5. Apparatus as claimed in claim 1 wherein the decoding means also detects any format command and provides an output to the disabling means to render the command ineffective.

6. Apparatus as claimed in claim 1, wherein the write protection device further comprises alarm means responsive to the comparator means for signalling an attempt to write to a write protected portion of the memory device.

7. Apparatus as claimed in claim 6 wherein the alarm means is also triggered by the detection of a format command by the decoding means.

8. Apparatus as claimed in claim 1, further comprising user-operated means for disabling the operation of the write protection device.

9. Apparatus as claimed in claim 1, wherein the disabling means includes logic switch means for preventing the write command from reaching the controller.

10. A write protection circuit for use with a computer having a CPU, a memory, and controller means for the memory, the write protection circuit comprising means for disabling write commands to the controller means which are addressed to preselected portions of the memory, characterised in that the write protection circuit is adapted to be connected between the CPU and the controller means.

11. A write protection circuit as claimed in claim 10, comprising decoding means for reading the address of any write command from the CPU to the controller of the memory; comparator means for comparing the write address with stored address(es) corresponding to portion(s) of the memory intended to be write protected; and disabling means responsive to the output of the comparator means for disabling write commands addressed to the stored address(es).

12. A write protection circuit as claimed in claim 10 further comprising means for disabling format commands.

13. A method of preventing unwanted writing of data to selected portion(s) of a memory device of a computer having a CPU and a controller for the memory device, comprising the steps of

(a) selecting the portion(s) of the memory device to which data is not intended to be written and storing the address(es) of the portion(s),

(b) reading the address of any write command from the CPU to the controller,

(c) comparing the write address with the stored address(es) of the preselected portion(s), and

(d) disabling those write commands having an address corresponding to the preselected portion(s),

characterised in that steps (b)-(d) are performed by a write protection device connected between the CPU and the controller.

14. A method as claimed in claim 13 further comprising the steps of detecting and disabling a format command to the controller.

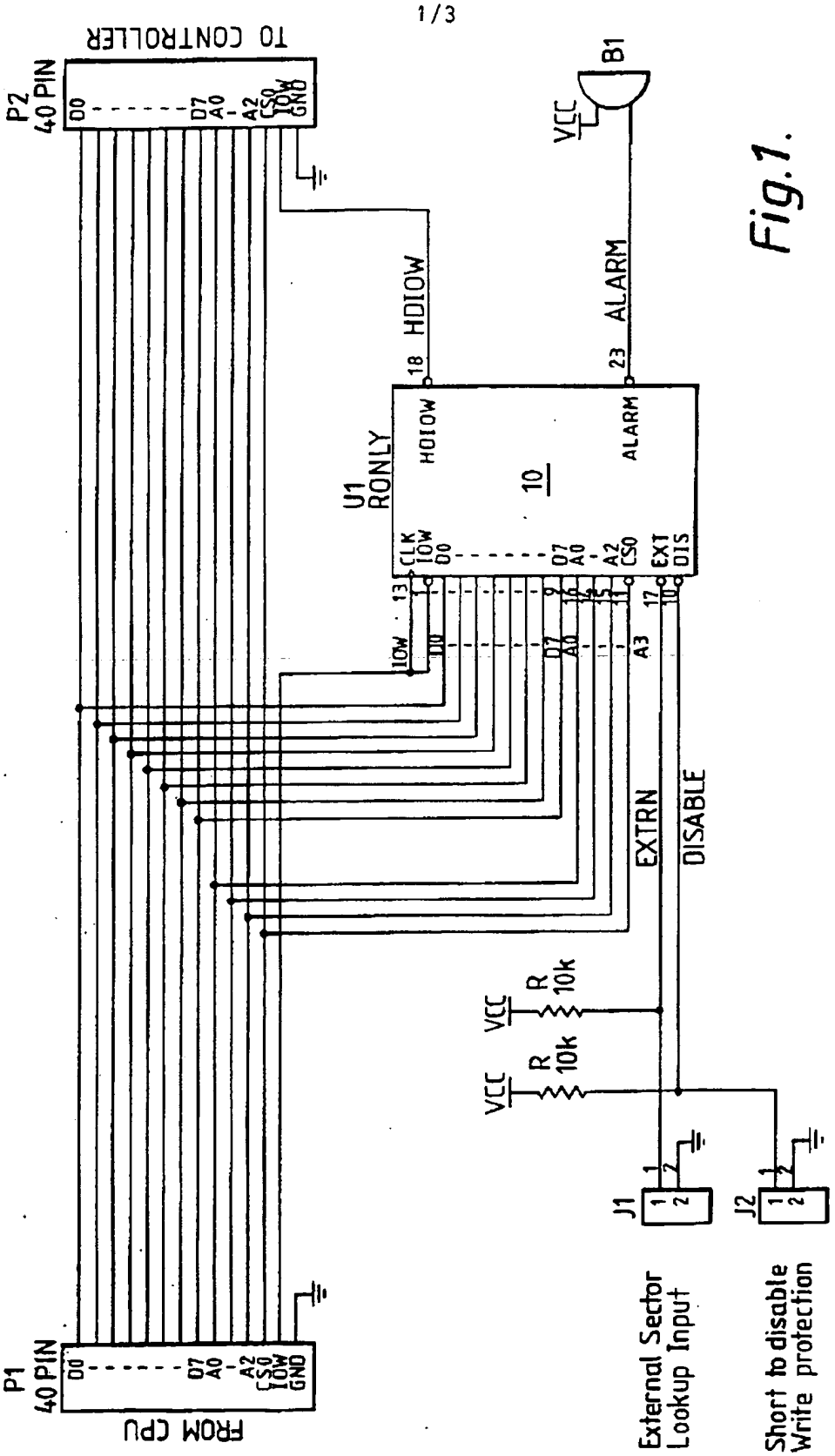

TO CONTROLLER
P2
40 PIN
D0
D7
A0
A2
CS0
IOW
GND
B1
VCC
ALARM
23
HDIOW
18
U1
RONLY
HDIOW
10
ALARM
CLK
IOW
D0
D7
A0
A2
CS0
EXT
DIS
13
IOW
D0
D7
A0
A3
17
EXTRN
DISABLE
R
10k
VCC
R
10k
VCC
J1
J2
External Sector
Lookup Input
Short to disable
Write protection
P1
40 PIN
D0
D7
A0
A2
CS0
IOW
GND
FROM CPU

Fig.1.

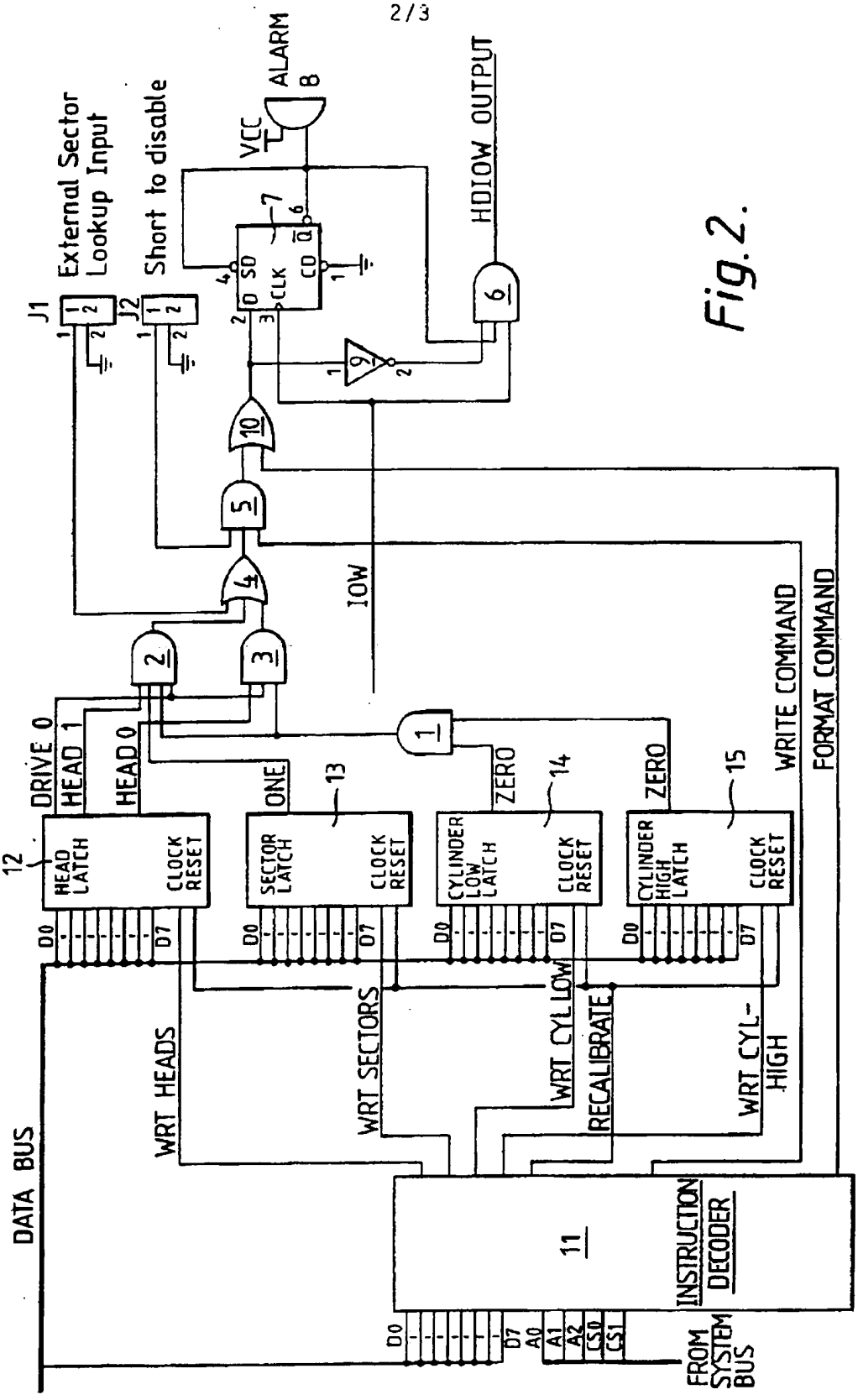

External Sector Lookup Input
Short to disable
ALARM
VCC
HDIOW OUTPUT
J1
J2
SD
CLK
CD
IOW
DRIVE 0
HEAD 1
HEAD 0
ONE
ZERO
ZERO
WRITE COMMAND
FORMAT COMMAND
HEAD LATCH
CLOCK RESET
SECTOR LATCH
CYLINDER LOW LATCH
CYLINDER HIGH LATCH
D0
D7
DATA BUS
WRT HEADS
WRT SECTORS
WRT CYL LOW
RECALIBRATE
WRT CYL-HIGH
INSTRUCTION DECODER
A0
A1
A2
CS0
CS1
FROM SYSTEM BUS

Fig. 2.

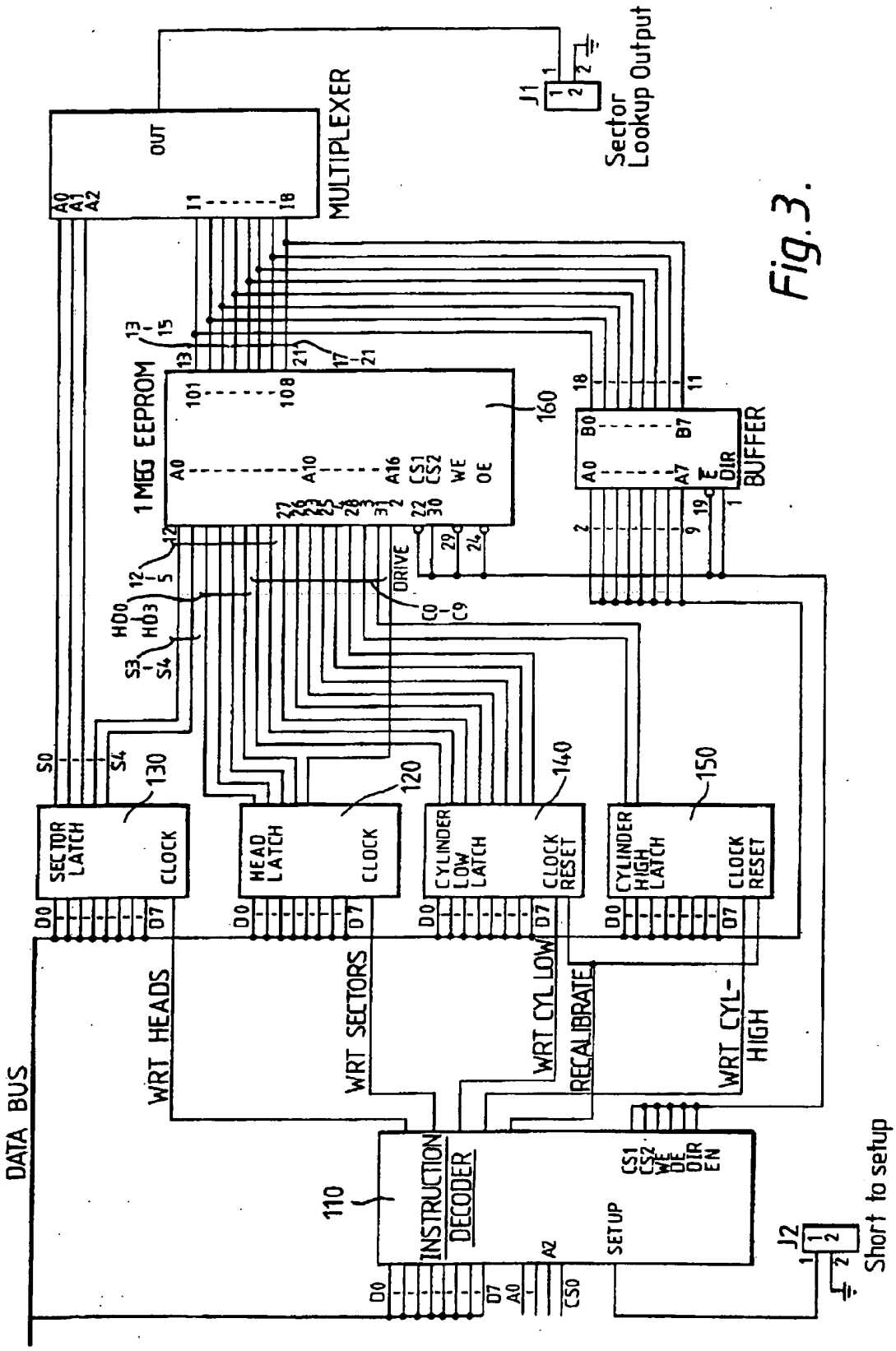

MULTIPLEXER
OUT
A0
A1
A2
J1
Sector Lookup Output
1 MEG EEPROM
160
A0
A10
A16
CS1
CS2
WE
OE
BUFFER
B0
B7
A7
DIR
DRIVE
C0-C9
HD0
HD3
S3
S4
S0
SECTOR LATCH
CLOCK
130
HEAD LATCH
120
CYLINDER LOW LATCH
CLOCK RESET
140
CYLINDER HIGH LATCH
150
D0
D7
DATA BUS
WRT HEADS
WRT SECTORS
WRT CYL LOW
RECALIBRATE
WRT CYL-HIGH
110
INSTRUCTION DECODER
SETUP
CS1
CS2
WE
OE
DIR
EN
A2
A0
CS0
J2
Short to setup

Fig. 3.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU92/00594

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl.[5] G06F 11/30, 12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC[5] G06F 11/30, 12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU IPC as above

Electronic data base consulted during the international search (name of data base, and where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
X,P	Patent abstract of Japan, P-1313, page 37, JP,A, 3-259359 (FUJITSU LTD) 19 November 1991 (19.11.91)	(1-14)
X	Patent abstract of Japan, P-786, page 139, JP,A, 63-163943 (YAMATAKE HONEYWELL CO LTD) 7 July 1988 (07.07.88)	(1-14)
Y,P	Patent abstract of Japan, P-1429, page 35, JP,A, 4-167038 (TOSHIBA CORP) 15 June 1992 (15.06.92)	(1-14)
Y	Patent abstract of Japan, P-1236, page 9, JP,A, 3-110620 (TOSHIBA CORP) 10 May 1991 (10.05.91)	(1-14)

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 February 1993 (03.02.93)	09 FEB 1993 (09-02-93)
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200 WODEN ACT 2606 AUSTRALIA Facsimile No. 06 2853929	Authorized officer J.W. THOMSON Telephone No. (06) 2832214

Form PCT/ISA/210 (continuation of first sheet (2)) (July 1992) copmeg

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate of the relevant passages	Relevant to Claim No.
Y	Patent abstract of Japan, P-964, Page 77, JP,A, 1-213733 (FUJITSU LTD) 28 August 1989 (28.08.89)	(1-14)
A,P	Patent abstract of Japan, P-1309, Page 108, JP,A, 3-252838 (FUJITSU LTD) 12 November 1991 (12.11.91)	
A	Patent abstract of Japan, P-504, page 112, JP,A, 61-112236 (TOSHIBA CORP) 30 May 1986 (30.05.86)	
Y	AU,A, 40995/89 (ROSE) 8 March 1990 (08.03.90)	(1-14)

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report	Patent Family Member
AU 40995/89	GB 2222899 US 5144660 ZA 8907831

END OF ANNEX